REMARKS

Claims 1-8, 10-39, 41-43, and 45-53 are pending in the present application. By this amendment, claims 1-8, 10-16, 19-31, 34-39, 41-43, 45, and 47 are amended, and claims 9, 40, and 44 are canceled without prejudice or disclaimer. Further, new claims 48-53 are added. Applicant respectfully requests reconsideration of the present claims in view of the above amendments and following remarks.

I. Allowable Subject Matter

Claims 14-15, 29-30, and 46-47 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the recitations of the base claims and any intervening claims. Accordingly, new independent claim 48 is added including at least the recitations of original claims 14, 13, 8, and base claim 1; new independent claim 50 is added including at least the recitations of original claims 29, 28, 22, and base claim 16; and new independent claim 52 is added including at least the recitations of original claims 46, 45, 37, and base claim 31. New claims 49, 51, and 53 are also added depending from new independent claims 48, 50, and 52, respectively. New claims 49, 51, and 53 include at least the recitations of original claims 15, 30, and 47. Therefore, Applicant respectfully asserts that new claims 48-53 are allowable over the cited art.

II. Claim Rejections Under 35 U.S.C. 102(a)

Claims 1-13, 16-28, and 31-45 are rejected under 35 U.S.C. §102(a) as being anticipated by the article entitled "Understanding Security Policies" to Cisco Systems, Inc. (hereinafter "Cisco"). As noted above, claims 9, 40, and 44 are canceled without prejudice or disclaimer, rendering this rejection moot with regard to those claims. Applicant respectfully traverses this rejection.

A. Claims 1-8 and 10-13 are allowable.

As amended, claim 1 recites that a system for providing network-based firewall policy configuration and facilitation associated with a firewall comprises a policy modification agent adapted to communicate with the firewall facilitation coordinator, the policy modification agent

configured to determine whether the application includes one or more questionable packets and to modify the user's firewall policy to allow at least a portion of the packets associated with the application to pass through the firewall unblocked, the at least a portion of the packets associated with the application determined based on whether the application includes one or more questionable packets.

Cisco does not teach, suggest, or describe a system for providing network-based firewall policy configuration and facilitation associated with a firewall as recited by claim 1. On the contrary, Cisco describes a firewall (Cisco Centri Firewall) operative to filter session attempts by evaluating the incoming request to start a new session against session controls and responses defined by a security policy to determine whether to allow the new session. Cisco further describes that the session controls used by the firewall to determine whether to allow a new session may be run-time session controls which are session controls that can be modified at the time the session request is received by the firewall.

This is not analogous to the system recited by claim 1 because Cisco fails to teach, suggest, or describe that the firewall is operative to determine whether the new session includes one or more questionable packets and to modify the security policy to allow at least a portion of the packets associated with the new session to pass through the firewall unblocked, where the portion of the packets allowed is determined based on whether the new session includes one or more questionable packets. Instead, Cisco describes that the firewall is operative to use session controls that can be modified at the time the session request is received by the firewall to determine whether to allow the new session as a whole, without teaching or suggesting that the firewall is operative to determine whether the new session includes one or more questionable packets and to modify the security policy to allow at least a portion of the packets of the new session, where the portion of the packets allowed is based on whether or not the new session includes questionable packets.

For at least the reasons given above, claim 1 is allowable over Cisco. Since claims 2-8 and 10-13 depend from claim 1 and recite further claim features, Applicant respectfully submits that Cisco does not anticipate Applicant's claimed invention as embodied in claims 2-8 and 10-13. Accordingly, Applicant respectfully requests withdrawal of these rejections.

B. Claims 16-28, 31-39, 41-43, and 45 are allowable.

As amended, claim 16 recites that a method for modifying a firewall policy of a network-based firewall comprises examining the packets traversing to/from the network-based firewall from/to the user to determine whether the new application includes one or more questionable packets and modifying the firewall policy to allow at least a portion of the packets associated with the new application to pass through the network-based firewall unblocked, the at least a portion of the packets associated with the new application determined based on whether the new application includes one or more questionable packets.

Cisco does not teach, suggest, or describe a method for modifying a firewall policy of a network-based firewall as recited by claim 16. In contrast, Cisco describes evaluating incoming requests to start a new session against session controls and responses defined by a security policy to determine whether to allow the new session. Cisco further describes that the session controls used to determine whether to allow a new session may be run-time session controls which are session controls that can be modified at the time the session request is received.

This is not analogous to the method recited by claim 16 because Cisco fails to teach, suggest, or describe examining packets associated with a new session traversing to/from the firewall from/to the user to determine whether the new session includes one or more questionable packets and modifying the security policy to allow at least a portion of the packets associated with the new session to pass through the firewall unblocked, where the portion of the packets associated with the new session allowed is determined based on whether the new session includes one or more questionable packets. Instead, Cisco describes using session controls that can be modified at the time the session request is received by the firewall to determine whether to allow the new session as a whole, without teaching or suggesting examining packets of the new session to determine whether the new session includes one or more questionable packets and modifying the security policy to allow at least a portion of the packets of the new session, where the portion of the packets allowed is based on whether or not the new session includes questionable packets.

For at least the reasons given above, claim 16 is allowable over Cisco. Since claims 17-28 depend from claim 16 and recite further claim features, Applicant respectfully submits that Cisco does not anticipate Applicant's claimed invention as embodied in claims 17-28. Accordingly, Applicant respectfully requests withdrawal of these rejections.

Independent claim 31 includes recitations similar to the recitations of claim 16. Thus, for at least the reasons given above with regard to claim 16, claim 31 is also allowable over Cisco. Since claims 32-39, 41-43, and 45 depend from claim 31 and recite further claim features, Applicant respectfully submits that Cisco does not anticipate Applicant's claimed invention as embodied in claims 32-39, 41-43, and 45. Accordingly, Applicant respectfully requests withdrawal of these rejections.

CONCLUSION

For at least these reasons, Applicant asserts that the pending claims 1-8, 10-39, 41-43, and 45-53 are in condition for allowance. Applicant further asserts that this response addresses each and every point of the Office Action, and respectfully requests that the Examiner pass this application with claims 1-8, 10-39, 41-43, and 45-53 to allowance. Should the Examiner have any questions, please contact Applicant's attorney at 404.815.1900.

Respectfully submitted,

HOPE BALDAUFF HARTMAN, LLC

Date: March 22, 2007

/Jodi L. Hartman/
Jodi L. Hartman
Reg. No. 55,251

Hope Baldauff Hartman, LLC
1720 Peachtree Street, NW
Suite 1010
Atlanta, Georgia 30309
Telephone: 404.815.1900